Integrated Public Alert and Warning System

Collaborative Operating Group Basics

Practitioner Special Interest Group

March 7, 2012

Agenda

1. Collaborative Operating Group Basics
2. Implications for Public Warning
3. MOA Security Requirements
4. MOA Notification Requirements
5. MOA Training Requirements
6. MOA Recordkeeping Requirements

Collaborative Operating Group Basics

- A Collaborative Operating Group (COG) is a virtual organization comprised of individual members that you rely or call upon for incident or disaster response

- A COG may be established at any geographic level sponsored by the appropriate government agency:
  - National
  - Multi-state
  - State
  - Multi-county
  - Single county
  - Single city or other local entity

- The purpose of a COG is to foster communication, collaboration, and coordination not only during the response phase, but also for preparedness, mitigation and recovery

Collaborative Operating Group Basics cont.

- One or more assigned COG Administrators create, manage, and update member accounts through their own software system
- COGs establish policy regarding who can be a member, including internal and external partners, i.e., “governance”
- The software system typically allows the administration of specific member permissions (e.g., create, update, delete, read only, etc.)

Collaborative Operating Group Basics cont.

- A COG may be established for the purpose of:
  - COG-to-COG alerting only--does not require state review
  - Both COG-to-COG alerting ***and*** public alerting via IPAWS dissemination systems (EAS, CMAS, HazCollect, future systems)--requires state review of separate IPAWS Public Alerting Application

- The software system should include the capability to administer user permission for "posting" to IPAWS, meaning the member can transmit alerts to IPAWS for :
  - delivery to other COGs and/or
  - delivery to the public via EAS, CMAS, HazCollect, or future systems

Implications for Public Warning

- Each COG is identified by a name and number that is associated with a digital certificate
- The digital certificate “signs” every CAP 1.2 alert message that is sent to IPAWS and ensures the identity of the originating COG (non-repudiation)
- The digital certificate is sent to the COG Point of Contact (POC) after the MOA process is completed via a secure method
- The COG POC coordinates directly with his software vendor to configure the software system with the digital certificate
- A list of system developers available from the FEMA Website indicates who has successfully tested digitally signing an alert http://www.fema.gov/pdf/emergency/ipaws/open_developers.pdf

Implications for Public Warning cont.

- Each state has its own set of laws regarding who is responsible for public warning
- In general, this authority is vested in a civilian elected official who may delegate to an emergency management or other agency
- If a state or local COG is established for the purpose of public alerting, then the state emergency management agency is asked by FEMA to identify a state reviewer to ensure consistency with state laws and relevant operational plans
- A separate public alerting application is completed by the applicant and sent to his designated state reviewer that includes:
  - Alert dissemination channels desired (EAS, CMAS, HazCollect)
  - Geographic extent of alerting authority by FIPS code
  - Specific non-weather event codes monitored by FCC participants (e.g. broadcasters) and/or used by CMAS

Implications for Public Warning – Options for State Systems

Some states may reserve all public warning authority at the state level and issue any local warnings on behalf of the local jurisdiction. Options to implement this arrangement through IPAWS may include:

- Local alerts are sent to the state for approval and posting to IPAWS via external means (e.g. email, fax, telephone, etc.)
- Local authorities are members of a state COG who have permission to author a public alert in a state-hosted system, but not to post to IPAWS for public dissemination
- Local authorities have their own COG ID and their own software but can only send alerts to the state COG for posting to IPAWS for public dissemination

Implications for Public Warning – Options for State Systems cont.

- A hybrid approach is used where local jurisdictions are authorized for public alerting as back up, and only used when the state system is not available

- Local authorities may be authorized for particular dissemination systems (e.g. CMAS, but not EAS) or particular event codes (e.g. not Child Abduction Emergency/CAE, typically reserved for state law enforcement agencies)

Implications for Public Warning – Options for Local Systems

In other states (especially "Home Rule" states) local jurisdictions have the authority to issue public warnings. Options to implement this arrangement through IPAWS may include:

- Local county (or equivalent) jurisdiction establishes a COG and manages alerting permissions for participating cities
- A city establishes its own COG and coordinates with other neighboring jurisdictions through COG-to-COG alerting
- A regional, multi-county, or multi-jurisdiction system COG is established under existing agreements, such as a Local Emergency Communications Committee (LECC) Emergency Alert System Plan

Implications for Public Warning – Options for Local Systems cont.

- A regional, multi-county or multi-jurisdiction COG is established under other existing plans such as Radiological Emergency Preparedness (REP) program or Chemical Stockpile Emergency Preparedness Program (CSEPP)
- Regional mutual aid organizations establish a single COG to align with mutual aid agreements or multi-agency coordination (MAC) systems

MOA Security Requirements – COG Members

- Official use only
- Official email accounts and equipment only
- Secure handling of configuration information (digital certificate)
- Discrete user account ID (no generic, shared accounts)
- Strong passwords, must be changed every 90 days
- Anti-virus software and regular scans
- Log-off or password protected screen saver when leaving workstation
- Promptly report IT security incidents, or any incidents of suspected fraud, waste or misuse of systems

FEMA

MOA Security Requirements – Sponsoring Organization

- Ensure Rules of Behavior are observed
- Digitally sign alerts
- System complies with all relevant federal laws, regulations and policies
- Provide physical security and system environmental safeguards
- Ensure physical and logical access is only granted to properly vetted and approved entities or individuals

FEMA

MOA Notification Requirements

- Immediate notice to FEMA when a security incident(s) is detected and/or a violation of the Rules of Behavior has been identified
- Immediate notice to FEMA if IPAWS access is no longer required
- Update contact information within 5 business days
- FEMA to provide notice to the COG of system disruptions

MOA Training Requirements

- Computer Security Awareness training prior to initial access and annually thereafter, either locally delivered course or if none is available, Domestic Preparedness Campus online course, CYBER 175-W (175-W) — Information Security for Everyone http://www.teexwmdcampus.com/wbtClass_info.k2?wbtClassID=108

- EMI IS-247 course for COG Point of Contact and any user with post permission for IPAWS public alerts http://training.fema.gov/EMIWeb/IS/is247.asp

- The COG Point of Contact must complete the EMI training and submit a copy of his/her training certificate as part of the application process. All other training records are maintained locally.

MOA Recordkeeping Requirements

- Document and maintain jurisdictional and/or system specific security policies and procedures and produce such documentation in response to official inquiries and/or requests.
- Signed Rules of Behavior Acknowledgements for COG members
- Training certificates

FEMA

Frequently Asked Questions

1. What type of sponsoring organizations are eligible to apply for a COG?
2. Is IPAWS mandatory for government agencies?
3. How do I find software?
4. Is grant funding available to purchase software or equipment?
5. Will I be notified when the MOA application process is complete?
6. How do I know when my software system is ready to use for COG-to-COG or public alerting?
7. Does IPAWS integrate with social media or use other generally available Internet services for dissemination.

Your Questions?

Comments and Questions

- **IPAWS Website -** http://www.fema.gov/emergency/ipaws

Antwane.Johnson@dhs.gov
Office: (202) 646-4383
Director, Integrated Public Alert and Warning System Division

Wade.Witmer@dhs.gov
Office: (202) 646-2523
Deputy Director, Integrated Public Alert and Warning System Division

Mark.Lucero@dhs.gov
Office: (202) 646-1386
Chief Engineering, Integrated Public Alert and Warning System Division

FEMA